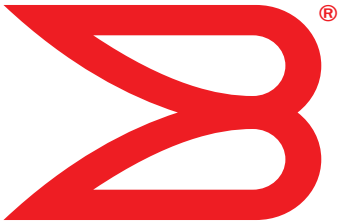
53-1002348-02
9 May 2012



Brocade 6910 Ethernet Access Switch

Diagnostic Guide

Supporting R2.1.0.x

BROCADE

Copyright © 2012 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, Brocade Assurance, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, MLX, NetIron, SAN Health, ServerIron, TurboIron, VCS, and VDX are registered trademarks, and AnyIO, Brocade One, CloudPlex, Effortless Networking, ICX, NET Health, OpenScript, and The Effortless Network are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit *http://www.brocade.com/support/oscd*.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
Brocade 6910 Ethernet Access Switch Diagnostic Guide	53-1002348-02	Updated information in the preface	May 2012
Brocade 6910 Ethernet Access Switch Diagnostic Guide	53-1002348-01	New document	September 2011

Contents

About This Document

Audience vii
Disclaimer vii
How to use this guide viii
Supported hardware viii
Document conventions viii
Text formatting ix
Command syntax conventions ix
Notes ix
Related publications x
Getting technical help x
Document feedback x

Chapter 1 Using Diagnostic Commands

How to use diagnostic commands 1
Console Connection 1
Show commands 1

Chapter 2 System and System Management Diagnostics

Basic system information 3
System hardware show commands 3
System software show commands 4
Common diagnostic scenarios 4
TCAM partitioning and usage 5
TCAM show commands 5
Configuration notes 5
Common diagnostic scenarios 6
Managing memory and CPU usage 6
CPU usage show command 6
CPU memory show command 7
Power supplies 7
Power supply show commands 7
Configuration notes 8
Common diagnostic scenarios 8
Fiber-optic modules 8
Fiber-optic show commands 9
Configuration notes 9

Testing network connectivity 10
Pinging an IP address 10
Tracing a route 11

Chapter 3 Layer 1 Diagnostics

Ethernet diagnostics 13
Duplex mismatches 13
Ethernet show commands 14
Common diagnostic scenarios 16

Chapter 4 Layer 2 Protocol Diagnostics

MAC address learning 19
Address Resolution Protocol 19
MAC address learning show commands 20
Spanning Tree Protocol and derivatives 20
STP 20
RSTP 20
MSTP 20
STP show commands 21
Configuration notes 24
Common diagnostic scenarios 24
LACP trunking 24
Trunk show commands 25
Configuration notes 26
Common diagnostic scenarios 26
VLAN trunking 27
VLAN trunking show commands 27
Ethernet Ring Protection switching 28
ERPS show commands 28
Connectivity Fault Management 28
CFM show commands 29
Operation, Administration and Maintenance 33
OAM show commands 33

Chapter 5 ACL and QoS Diagnostics

ACLs 37
ACL show commands 37
Common diagnostic scenarios 37
QoS 38
QoS show commands 38

Chapter 6 Security Diagnostics

802.1x 41
802.1x show commands 41
Configuration notes 43

Port loop detection 44
Port loop detection show commands 44
Configuration notes 44
Port mirroring and monitoring 45
Port mirroring show commands 45
RADIUS. 45
RADIUS show commands 46
Configuration notes 47
SNMP 47
SNMP show commands. 47
Configuration notes 49
TACACS and TACACS+ 49
TACACS+ show commands 49
Configuration notes 50
Telnet and SSH connections 51
Telnet and SSH show commands 51
Configuration notes 51
SNTP. 52
SNTP show commands 52

Chapter 7 Forwarding Diagnostics

Trunking 53
Trunking show commands. 53
Configuration notes 55
Common diagnostic scenarios 55

Diagnostic Command Index

About This Document

This manual describes troubleshooting and diagnostic commands available in the command line interface (CLI) for the Brocade Ethernet Access Switch.

NOTE
Some troubleshooting commands report information about internal hardware settings and registers that is relevant primarily to the Brocade engineering staff. Consequently, this information is not described in this document.

Audience

This document is designed for system administrators with a working knowledge of Layer 2 and Layer 3 switching and routing.

Disclaimer

This manual is provided without any warranty of any kind, expressed or implied. When using this manual to troubleshoot Brocade products, you assume all risk as to the quality and performance of the diagnostic procedures. Brocade assumes no liability for any damages, including general, special, incidental, or consequential damages arising from the use of the diagnostic procedures in this manual (including, but not limited to, any loss of profit or savings, loss of data, or failure to successfully troubleshoot network problems).

Diagnostic information may be changed or updated without notice. You are responsible for obtaining newer versions of this manual when they are made available. The procedures in this document are not intended as a substitute for the expertise of qualified technicians.

Enabling diagnostic commands can seriously degrade system performance. Diagnostic commands are generally intended for use when troubleshooting specific problems while working with qualified service technicians, or in conjunction with calls to Brocade Technical Support. Whenever possible, troubleshoot your system during periods of low network traffic and user activity to preserve system performance.

If you have any questions regarding this Disclaimer, please contact us at support@brocade.com.

How to use this guide

This guide describes many common diagnostic processes for the Brocade BR6910 switch. Each chapter contains diagnostic information about a specific segment of your network configuration. Each topic consists of the following sections, where possible, and when the information is applicable:

- A brief description of the topic
- Show commands related to the topic
- Configuration notes for the topic
- Common diagnostic scenarios

Supported hardware

The following hardware platforms are supported by the release of this guide:

- BR-6910-EAS-AC – Brocade 6910 Ethernet Access Switch, 12×1 GbE combination copper 10/100/1000 Base-T (RJ45) or 100/1000 Base-X SFP ports, redundant AC power supply
- BR-6910-EAS-DC – Brocade 6910 Ethernet Access Switch, 12×1 GbE combination copper 10/100/1000 Base-T (RJ45) or 100/1000 Base-X SFP ports, redundant DC power supply
- BR-6910-EAS-H-AC – Brocade 6910 Ethernet Access Switch, 12×1 GbE combination copper 10/100/1000 Base-T (RJ45) or 100/1000 Base-X SFP ports, redundant AC power supply, temperature hardened
- BR-6910-EAS-H-DC – Brocade 6910 Ethernet Access Switch, 12×1 GbE combination copper 10/100/1000 Base-T (RJ45) or 100/1000 Base-X SFP ports, redundant DC power supply, temperature hardened

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names
	Identifies the names of user-manipulated GUI elements
	Identifies keywords
	Identifies text to enter at the GUI or CLI
italic text	Provides emphasis
	Identifies variables
	Identifies document titles
`code` text	Identifies CLI output

Command syntax conventions

Command syntax in this manual follows these conventions:

command	Commands are printed in bold.
--**option, option**	Command options are printed in bold.
-**argument,** arg	Arguments.
{ }	Mandatory elements appear in braces.
[ ]	Optional elements appear in brackets.
variable	Variables are printed in italics.
...	Repeat the previous element, for example “member[,member...]”
value	Fixed values following arguments are printed in plain font. For example, --**show** WWN
|	Boolean. Elements are exclusive. Example: --**show** -**mode** egress | ingress

Notes

The following notice statements are used in this manual.

NOTE
A note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates potential damage to hardware or data.

Related publications

The following Brocade Communications Systems, Inc. documents supplement the information in this guide and can be located at *http://www.brocade.com/ethernetproducts.*

- *Brocade 6910 Ethernet Access Switch Installation Guide*
- *Brocade 6910 Ethernet Access Switch MIB Reference*
- *Brocade 6910 Ethernet Access Switch Diagnostic Guide*

NOTE
For the latest edition of these documents, which contain the most up-to-date information, see Product Manuals at http://www.brocade.com/ethernetproducts.

Getting technical help

To contact Technical Support, go to *http://www.brocade.com/services-support/index.page* for the latest e-mail and telephone contact information.

Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Chapter

1

Using Diagnostic Commands

How to use diagnostic commands

This chapter describes how to use Brocade diagnostic show commands to monitor and troubleshoot the Brocade 6910 switch configuration. Show commands are accessible from the Privileged Exec mode in the command line interface (CLI). Some show commands can be configured to send output to a destination that you specify.

Many show commands are specifically designed to be used in conjunction with calls to Brocade Technical Support. If you report a problem, the support engineer may ask you to execute one or more of the diagnostic commands described in this guide.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are “admin” and “guest” with corresponding passwords of “admin” and “guest.”) When the administrator user name and password is entered, the CLI displays the “Console#” prompt and enters privileged access mode (i.e., Privileged Exec). When the guest user name and password is entered, the CLI displays the “Console>” prompt and enters normal access mode (i.e., Normal Exec).
2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the “quit” or “exit” command.

Show commands

Show commands provide information that is extremely helpful for troubleshooting. For most of the environments discussed in this document, related show commands, show command output, and output descriptions are included.

Many show commands generate output for a specific configuration.

show log

Syntax: show log {**flash** | **ram**}

The **show log** command allows you to view the system log. Command output similar to the following is displayed.

```
Console# show logging ram
Syslog logging               : Enabled
History logging in RAM       : Level debugging
```

```
Console# show log ram
[9] 10:40:35 2011-04-15
   "User(admin/Console), login successful."
   level : 6, module : 5, function : 1, and event no. : 1
[8] 08:25:27 2011-04-15
   "User(admin/Console), login successful."
   level : 6, module : 5, function : 1, and event no. : 1
[7] 08:25:17 2011-04-15
   "DHCP server responded."
   level : 5, module : 9, function : 1, and event no. : 11
[6] 08:25:17 2011-04-15
   "STA topology change notification."
   level : 6, module : 5, function : 1, and event no. : 1
[5] 08:25:15 2011-04-15
   "STP port state: MSTID 0, Eth 1/1 becomes forwarding."
   level : 6, module : 5, function : 1, and event no. : 1
[4] 08:25:15 2011-04-15
   "VLAN 1 link-up notification."
   level : 6, module : 5, function : 1, and event no. : 1
[3] 08:25:14 2011-04-15
   "Unit 1, Port  1 link-up 100M FD notification."
   level : 6, module : 5, function : 1, and event no. : 1
[2] 08:25:10 2011-04-15
   "System coldStart notification."
   level : 6, module : 5, function : 1, and event no. : 1
[1] 08:25:09 2011-04-15
   "CPU falling trap."
   level : 6, module : 5, function : 1, and event no. : 1
[0] 08:24:59 2011-04-15
   "CPU rising trap."
   level : 6, module : 5, function : 1, and event no. : 1
```

Chapter

System and System Management Diagnostics 2

This chapter describes many of the common system and system management diagnostic processes for Brocade 6910 switch.

Basic system information

Basic system troubleshooting includes the verification of software images and their locations, and monitoring hardware components such as power supplies. The following sections describe how to display information, and what to look for when troubleshooting your hardware and system software.

System hardware show commands

show system

Syntax: show system

The **show system** command displays system information about the chassis, including primary and redundant power supplies. The following example shows output for the **show system** command.

```
Console# show system
System Description : BR6910
System OID String  : 1.3.6.1.4.1.1991.1.16.1
System Information
 System Up Time          : 0 days, 4 hours, 27 minutes, and 30.58 seconds
 System Name             :
 System Location         :
 System Contact          :
 MAC Address (Unit 1)    : 70-72-CF-32-DD-FD
 Web Server              : Enabled
 Web Server Port         : 80
 Web Secure Server       : Enabled
 Web Secure Server Port  : 443
 Telnet Server           : Enabled
 Telnet Server Port      : 23
 Jumbo Frame             : Disabled

System Temperature:
Unit 1
 Temperature 1: 28 degrees  Temperature 2: 26 degrees  Temperature 3: 26 degrees

 Main Power Status       : Up
 Redundant Power Status  : Up
```

show alarm-status

Syntax: show alarm-status

This command displays information on predefined alarms (i.e., non-configurable) and on the link-down alarm (which is displayed as a minor alarm).

```
Console# show alarm-status
Unit 1
Asserted Alarm Input : [NONE]
Current Major Alarm Status:
One of the power status is failed.
Current Minor Alarm Status:[NONE]
Current Major Alarm Output Status:[ACTIVE]
Current Minor Alarm Output Status:[INACTIVE]
```

System software show commands

show version

Syntax: show version

Most boot issues occur because incorrect or incompatible images have been downloaded. The **show version** command displays all versions that are currently loaded, as shown in the following example.

```
Console# show version
Unit 1
 Serial Number          : S123456
 Hardware Version       : R0A
 EPLD Version           : 0.00
 Number of Ports        : 12
 Main Power Status      : Up
 Redundant Power Status : Up
 Role                   : Master
 Loader Version         : 0.0.0.5
 Linux Kernel Version   : 2.6.22.18
 Boot ROM Version       : 0.0.0.1
 Operation Code Version : 0.0.1.6
```

Common diagnostic scenarios

System issues are rare. However, some problem sources can include:

- Software versions are not compatible.
- Environmental conditions, such as temperatures that are above or below operating thresholds, are affecting operation of hardware components.

If you are experiencing system issues, contact Brocade Technical Support for help in troubleshooting your system.

TCAM partitioning and usage

Ternary Content Addressable Memory (TCAM) is a component of Brocade devices that facilitates hardware forwarding. As packets flow through the Brocade device from a given source to a given destination, the management processor records forwarding information about the flow in TCAM entries. A TCAM entry generally contains next-hop information, such as the outgoing port, the MAC address of the next-hop router, a VLAN tag, and so on. Once the Brocade device has this information in TCAM, packets with the same source and destination can be forwarded by hardware, bypassing the management processor, and speeding up forwarding time.

TCAM stores Layer 2, Layer 3, or Layer 4 information in policy control entries. These entries are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, or traps. For example, when binding an ACL to a port, each rule in an ACL will use two policy control entries; and when setting an IP Source Guard filter rule for a port, the system will also use two policy control entries.

TCAM show commands

show access-list tcam-utilization

Syntax: show access-list tcam-utilization

This command shows utilization parameters for TCAM, including the number policy control entries in use, the number of free policy control entries, and the overall percentage of TCAM in use.

NOTE
The total number of policy control entries is fixed at 640, and cannot be configured.

```
Console# show access-list tcam-utilization
  Total Policy Control Entries : 640
  Free Policy Control Entries  : 522
  Entries Used by System       : 118
  Entries Used by User         : 0
  TCAM Utilization             : 18.43%
```

Configuration notes

The Brocade 6910 switch can have up to 512 static and dynamic MAC addresses stored in the TCAM (using two policy control entries per address). The ability of the TCAM to store large numbers of addresses depends on the following factors:

- The number of source MAC addresses being learned by the TCAM.
- The number of destination MAC addresses being forwarded by the TCAM.
- The distribution of the MAC address entries across ports. For example, if one port is learning all the source MAC addresses, the available TCAM will be used up by that port. In addition, a large number of MAC address entries in the MAC table could increase CPU use.
- The TCAM provides a total of 1000 hardware entries. However, each rule used by the system for basic functions or configured by the user requires two policy control entries. Some entries are used by the system for basic functions, L3 lite functions (including static routing and automatic routing between directly-connected Layer 3 interfaces), web authentication, IP Source Guard, and any configured ACL rules.

Common diagnostic scenarios

When troubleshooting TCAM issues, it is helpful to know when a device is running out of TCAM. The following sections describe how to monitor TCAM usage.

Displaying TCAM settings

When a Brocade device boots, the system automatically sets default TCAM partitions.

The default TCAM settings are the same as the default partition percentage settings.

NOTE
The default TCAM partitions are fixed, and cannot be configured.

Determining if a device is running out of TCAM

The output of the **show access-list tcam-utilization** command will indicate if the device is running out of TCAM.

Managing memory and CPU usage

To achieve maximum performance, it is important to understand CPU usage and memory issues in the Brocade 6910 switches. The following sections discuss how to manage memory and CPU usage.

The first step in determining how your device is using memory and the CPU is to get a view of the activity. Several show commands display information about CPU usage and memory usage.

CPU usage show command

There is one command that shows the overall usage of the CPU, and the configured thresholds used for sending an SNMP trap message.

show process cpu

Syntax: show process cpu

The **show process cpu** command displays overall CPU usage and alarm message thresholds, as shown in the following example.

```
Console# show process cpu
 CPU Utilization in the past 5 seconds : 19%

 CPU Utilization in the past 60 seconds
  Average Utilization      : 16%
  Maximum Utilization      : 21%

 Alarm Status
  Current Alarm Status     : Off
  Last Alarm Start Time    : Jun 17 07:42:29 2011
  Last Alarm Duration Time : 20 seconds

 Alarm Configuration
  Rising Threshold         : 90%
  Falling Threshold        : 70%
```

CPU memory show command

The CPU uses memory buffers to handle interprocess communication (IPC) and external packets sent and received by the management processor.

show memory

Syntax: show memory

The **show memory** command shows the amount of memory currently free for use, the amount of memory allocated to active processes, and the total amount of system memory, and the configured thresholds used for sending an SNMP trap message, as shown in the following example.

```
Console# show memory
 Status Bytes      %
 ------ ---------- ---
 Free     34775040  25
 Used     99442688  75
 Total   134217728

 Alarm Configuration
  Rising Threshold         : 90%
  Falling Threshold        : 70%
```

Power supplies

Information about power supplies can be displayed.

Power supply show commands

show system

Syntax: show system

You can view power supply information using the **show system** command. Command output resembles the following example. (The temperatures shown by this command are in Celsius.)

```
Console# show system
System Description : BR6910
System OID String  : 1.3.6.1.4.1.1991.1.16.1
System Information
 System Up Time          : 0 days, 4 hours, 37 minutes, and 26.11 seconds
 System Name             :
 System Location         :
 System Contact          :
 MAC Address (Unit 1)    : 70-72-CF-32-DD-FD
 Web Server              : Enabled
 Web Server Port         : 80
 Web Secure Server       : Enabled
 Web Secure Server Port  : 443
 Telnet Server           : Enabled
 Telnet Server Port      : 23
 Jumbo Frame             : Disabled

System Temperature:
Unit 1
 Temperature 1: 28 degrees  Temperature 2: 26 degrees  Temperature 3: 26 degrees
```

```
Main Power Status      : Up
Redundant Power Status : Up
```

Configuration notes

There are several cautions and warnings that you should pay attention to when installing or replacing power supplies. Refer to the *Brocade BR6910 Installation Guide* for more information.

Common diagnostic scenarios

- Power supply is not providing power - check all power connections, and replace faulty power supply if necessary. See the *Bro a dc om BR6910 Installation Guide* for more information.
- Temperature is outside normal operating range. See the following section.

What to do if the temperature is outside normal operating range

If the device detects temperatures outside the normal range, depending on the severity of the reading, it will automatically do one of the following:

- Leave the fan speed as is.
- Increase the fan speed.
- Decrease the fan speed.
- Generate a Syslog message and an SNMP trap.

If none of these measures resolves the problem, you should perform the following steps:

1. Shut down the device immediately.
2. Inspect all fans for damage or failure.
3. Inspect electrical connections to the fans.
4. Contact technical support at Brocade for assistance.

The normal operating temperature, humidity, and altitude specifications for Bro a dc om 6910 Switch are:

- Operating Temperature: -40° – 149° F (-40° – 65° C).
- Relative Humidity: 5 to 90%, @ 149° F (65° C), non-condensing.
- Operating Altitude: 0 – 10,000 ft (0 – 3048 meters).

Fiber-optic modules

The most common problems with fiber-optic modules are caused by dirty connectors. Optical cables that are contaminated in any way (with dust, hand oil, and so on) can degrade the optic eye pattern. Some of the following symptoms may be experienced:

- Port appears not to function (either no link or unstable link)
- Cyclic redundancy check (CRC) errors
- Port flapping

- Packet loss

Before inserting the fiber cable into the fiber-optic transceiver, ensure that it is free of dust by cleaning the end. A “Fiber Swiper” cleaner is provided by Brocade for this purpose with each optic shipment (reference instructions provided with the Fiber Swiper).

It is very important that the end of an optical cable is clean when using any data rate. This must be the first step in troubleshooting symptoms such as those stated previously. Always ensure that the optical cables are cleaned.

NOTE
When not using a fiber-optic module port connector, replace the protective cover to prevent dust or dirt from contaminating the connector.

Fiber-optic show commands

show interfaces transceiver

Syntax: show interfaces transceiver [**ethernet** *unit/port*]

This command displays information about optic modules installed in the Brocade 6910 switches. Optics information resembles the output segment in the following example.

```
Console# show interfaces transceiver ethernet 1/1
Information of Eth 1/1
 Connector Type        : LC
 Fiber Type            : Multimode 50um (M5), Multimode 62.5um (M6)
 Eth Compliance Codes  : 1000BASE-SX
 Baud Rate             : 1200 MBd
 Vendor OUI            : 00-30-D3
 Vendor Name           : AGILENT
 Vendor PN             : HFBR-5710L
 Vendor Rev            :
 Vendor SN             : 0111010843570877
 Date Code             : 01-11-01
 DDM Info
   Not support DDM
```

Configuration notes

Before installing or removing fiber optic modules, refer to the precautions and follow the instructions in the *Brocade 6910 Installation Guide*.

Testing network connectivity

You can test connectivity to other network devices by pinging those devices. You also can trace routes.

Pinging an IP address

To verify that a Brocade 6910 switch can reach another device through the network, enter the **ping** command at the Normal Exec or Privileged Exec level of the CLI, or enter the **ping6** command at the Privileged Exec level of the CLI.

ping

Syntax: **ping** {*ipv4-addr* | *hostname*} [**count** *num*] [**size** *byte*]

- *ipv4-addr* - Specifies the IP address of the device.
- *hostname* - Specifies the host name.
- **count** *num* - Specifies how many ping packets the device sends.
- **size** *byte* - Specifies the size of the ICMP data portion of the packet.

NOTE
If you address the ping to the IP broadcast address, the device lists the first four responses to the ping.

ping6

Syntax: **ping6** {*ipv6-addr* | *hostname*} [**count** *num*] [**size** *byte*]

- *ipv6-addr* - Specifies the IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373, “IPv6 Addressing Architecture,” using eight colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

  NOTE
  The same link-local address may be used by different interfaces or nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone ID information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.

- *hostname* - Specifies a host name string that can be resolved into an IPv6 address through a domain name server.
- **count** *num* - Specifies how many ping packets the device sends.
- **size** *byte* - Specifies the size of the ICMP data portion of the packet.

Tracing a route

To determine the path through which the router can reach another network device, enter the **traceroute** command at the Privileged Exec level of the CLI.

traceroute

Syntax: traceroute {*ipv4-addr* | *hostname*}

- *ipv4-addr* - Specifies the IP address of the device.
- *hostname* - Specifies the host name.

The CLI displays trace route information for each hop as soon as the information is received. A trace terminates when the destination responds, when the time-to-live (TTL) is exceeded, or the maximum number of hops is exceeded.

Chapter

Layer 1 Diagnostics 3

This chapter describes common Layer 1 diagnostic procedures for the Brocade 6910 series switches. In general, Layer 1 issues are related to hardware, the most common being the following physical connectivity problems:

- Faulty ports
- Faulty cables
- Faulty hardware
- Input and output errors
- Cyclic redundancy check (CRC) errors
- Excessive or late collisions
- Overruns
- Output buffer failures

Ethernet diagnostics

The following sections describe how to troubleshoot Layer 1 issues for Ethernet interfaces.

Duplex mismatches

A duplex mismatch can occur between devices in the following situations:

- One device is manually set to half duplex and one device is manually set to full duplex.
- One device is set to autonegotiation and one device is manually set to full duplex.

Duplex mismatches are difficult to diagnose because the network still appears to be working. Simple tests, such as ping, report a valid connection even though network performance can be much slower than normal.

When one device operates in full duplex while the other one operates in half duplex, the connection works at a very low speed if both devices attempt to send frames at the same time. This is because a full-duplex device may transmit data while it is receiving, but if the other device is working in half duplex, it cannot receive data while it is sending. The half-duplex device senses a collision and attempts to resend the frame it was sending. Depending on timing, the half-duplex device may sense a late collision, which it will interpret as a hard error, and will not attempt to resend the frame. At the other end, the full-duplex device does not detect a collision and does not resend the frame, even if the half-duplex device has already discarded it as corrupted by collision.

The packet loss happens when both devices are transmitting at the same time, and may happen even when the link is used, from the user's perspective, in one direction only. A Transmission Control Protocol (TCP) stream requires that all packets sent be acknowledged by the receiving device, even if actual data is sent in one direction only. Packet collisions may occur with acknowledgement packets traveling in the other direction.

Because the full-duplex device does not expect incoming frames to be truncated by collision detection, the device reports Frame Check Sequence (FCS) errors. The combination of late collisions reported at the half-duplex end, and FCS errors reported by the full-duplex end, can indicate a duplex mismatch.

Ethernet show commands

This section describes the show commands that display information about Ethernet interfaces.

show interfaces brief

Syntax: show interfaces brief

This command displays a summary of the information provided in the **show interfaces** command. Command output resembles the following example.

```
Console# show interfaces brief
Interface Name               Status   PVID Pri Speed/Duplex  Type         Trunk
--------- ------------------ -------- ---- --- ------------- ------------ -----
Eth 1/ 1                     Up          1   0 Auto-100full  1000T        None
Eth 1/ 2                     Down        1   0 Auto          1000Base SFP None
```

show interfaces counters ethernet

Syntax: show interfaces counters ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

This command displays statistics about a specific Ethernet interface, as shown in the following example.

```
Console# show interfaces counters ethernet 1/1
Ethernet 1/ 1
 ===== IF table Stats =====
                1562954 Octets Input
                5265175 Octets Output
                   5389 Unicast Input
                   6254 Unicast Output
                      0 Discard Input
                      0 Discard Output
                      0 Error Input
                      0 Error Output
                      0 Unknown Protos Input
                      0 QLen Output
 ===== Extended Iftable Stats =====
                  10446 Multi-cast Input
                  11128 Multi-cast Output
                    313 Broadcast Input
                      2 Broadcast Output
 ===== Ether-like Stats =====
                      0 Alignment Errors
                      0 FCS Errors
                      0 Single Collision Frames
                      0 Multiple Collision Frames
                      0 SQE Test Errors
                      0 Deferred Transmissions
                      0 Late Collisions
                      0 Excessive Collisions
                      0 Pause Frames Output
```

```
===== RMON Stats =====
                     0 Drop Events
                10305324 Octets
                   32060 Packets
                     270 Broadcast PKTS
                    9075 Multi-cast PKTS
                       0 Undersize PKTS
                       0 Oversize PKTS
                       0 Fragments

                       0 Internal Mac Transmit Errors
                       0 Internal Mac Receive Errors
                       0 Frames Too Long
                       0 Carrier Sense Errors
                       0 Symbol Errors
                       0 Pause Frames Input
```

show interfaces status ethernet

Syntax: show interfaces status ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

This command displays the operational status for Ethernet ports, as shown in the following example.

```
Console# show interfaces status ethernet 1/1
Information of Eth 1/1
 Basic Information:
  Port Type              : 1000BASE-T
  MAC Address            : 70-72-CF-32-DD-FE
 Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm        : Enabled
  Broadcast Storm Limit  : 64 Kbits/second
  Multicast Storm        : Disabled
  Multicast Storm Limit  : 64 Kbits/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 64 Kbits/second
  Flow Control           : Disabled
  VLAN Trunking          : Disabled
  LACP                   : Disabled
  Port Security          : Disabled
  Max MAC Count          : 0
  Port Security Action   : None
  Media Type             : SFP preferred auto
 Current Status:
  Link Status            : Up
  Port Operation Status  : Up
  Operation Speed-duplex : 100full
  Up Time                : 0w 0d 5h 51m 29s (21089 seconds)
  Flow Control Type      : None
```

show interfaces switchport ethernet

Syntax: show interfaces switchport ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

This command displays the administrative and operational status for Ethernet ports, as shown in the following example.

```
Console# show interfaces switchport ethernet 1/1
Information of Eth 1/1
 Broadcast Threshold           : Enabled, 64 Kbits/second
 Multicast Threshold           : Disabled
 Unknown Unicast Threshold     : Disabled
 LACP Status                   : Disabled
 Ingress Rate Limit            : Disabled, 64 Kbits per second
 Egress Rate Limit             : Disabled, 1000000 Kbits per second
 VLAN Membership Mode          : Hybrid
 Ingress Rule                  : Disabled
 Acceptable Frame Type         : All frames
 Native VLAN                   : 1
 Priority for Untagged Traffic : 0
 GVRP Status                   : Disabled
 Allowed VLAN                  :     1(u)
 Forbidden VLAN                :
 802.1Q Tunnel Status          : Disabled
 802.1Q Tunnel Mode            : Normal
 802.1Q Tunnel TPID            : 8100 (Hex)
 Layer 2 Protocol Tunnel       : None
```

Common diagnostic scenarios

The following issues can occur with Ethernet interfaces:

- Faulty hardware

  Whenever you encounter a connection problem, check for faulty hardware. Replace cables, try another port, and check all cable connections. If you find a faulty port, contact Brocade Technical Support for assistance.

- Link failures

  Link failures can be due to a failure of the transmission medium or of the devices at each end of a connection. Be sure to check all of the hardware involved in the link, including cables and ports.

- CSMA/CD

  The Carrier Sense Multiple Access (CSMA) with Collision Detection (CD) protocol controls access to shared Ethernet media. A switched network (for example, Fast Ethernet) may use a full-duplex mode with access to the full link speed between directly connected network interface cards (NICs), switch-to-NIC cables, or switch-to-switch cables.

- CRC errors

  The Cyclic Redundancy Check (CRC) length specifies whether the CRC portion of each frame transmitted on the interface is 16 bits or 32 bits long. The default is 32 bits.

A CRC alignment error is generated when the total number of packets received is from 64 through 1518 octets, but contains either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a non-integral number of octets (alignment error).

- Runts

  Any received packet that is less than 64 bytes is illegal, and is called a runt. In most cases, runts arise from a collision, and although they indicate an illegal reception, they may occur on correctly functioning networks. The receiving Brocade device discards all runt frames.

- Giants

  Any received packet that is greater than the maximum frame size is called a giant. In theory, the jabber control circuit in the transceiver must prevent any node from generating such a frame, but certain failures in the physical layer may also give rise to oversized Ethernet frames. Like runts, giants are discarded by the receiving Brocade device.

- Misaligned frames

  Any frame that does not contain an integral number of received octets (bytes) is also illegal. A receiver has no way of knowing which bits are legal, and how to compute the CRC-32 of the frame. Such frames are therefore also discarded by the receiving Brocade device.

NOTE
Brocade recommends regular software maintenance and upgrades to keep up with firmware code updates.

Chapter

Layer 2 Protocol Diagnostics

4

This chapter describes Layer 2 troubleshooting and diagnostic processes for the Brocade 6910 switch.

MAC address learning

In MAC address learning, the source MAC address of each received packet is stored so that future packets destined for that address can be forwarded only to the interface where that address is located. (Packets destined for unrecognized addresses are forwarded out every bridge interface.) MAC address learning, defined in the IEEE 802.1 standard, helps minimize traffic on the attached LANs.

Address Resolution Protocol

Switches use Address Resolution Protocol (ARP) to learn the MAC addresses of devices on the network. The switch sends an ARP request that contains the IP address of a device, and receives the MAC address for that device in an ARP reply. These dynamically learned entries are stored in the ARP cache. You can also manually configure MAC addresses, which are called static entries.

Dynamic and static ARP entries in the ARP cache resemble the following:

```
Console# show arp
ARP Cache Timeout: 1200 (seconds)

IP Address      MAC Address       Type      Interface
--------------- ----------------- --------- -----------
192.168.0.2     74-8E-F8-68-02-30 other     VLAN1
192.168.0.9     11-22-33-44-55-66 static    VLAN1
192.168.0.99    00-E0-29-94-34-64 dynamic   VLAN1

Total entry : 3
```

ARP age

The ARP age is the amount of time the device keeps a learned MAC address in the ARP cache. The device resets the timer to zero each time the ARP entry is refreshed and removes the entry if the timer reaches the ARP age. The default ARP age is 20 minutes.

Changing the ARP aging period

When the switch places an entry in the ARP cache, it also starts an aging timer for the entry. The aging timer ensures that the ARP cache does not retain learned entries that are no longer valid. An entry can become invalid when the device with the MAC address of the entry is no longer on the network.

ARP age affects dynamic entries only.

MAC address learning show commands

The following command displays information about the MAC address table.

show mac-address-table

Syntax: show mac-address-table

This command displays the MAC address table, which contains MAC addresses learned from other devices. This table does not contain the MAC addresses of the Brocade device ports.

```
Console# show mac-address-table

 Total entry in system: 3
 Interface MAC Address       VLAN Type     Life Time
 --------- ----------------- ---- -------- -----------------
  CPU      70-72-CF-32-DD-FD    1 CPU      Delete on Reset
  Eth 1/ 1 00-01-EC-F8-D8-D6    1 Learn    Delete on Timeout
  Eth 1/ 1 00-E0-29-94-34-64    1 Learn    Delete on Timeout
```

Spanning Tree Protocol and derivatives

The following sections describe diagnostic procedures for Spanning Tree Protocol (STP) and STP derivatives, including RSTP and MSTP.

NOTE
Layer 2 protocols such as STP and RSTP can be enabled on port-based VLANs, but cannot be enabled or disabled on protocol-based VLANs.

STP

A control protocol, such as Spanning Tree Protocol (STP), can block one or more ports in a protocol-based VLAN that uses a virtual routing interface to route to other VLANs. For IP VLANs and IP subnet VLANs, even though some of the physical ports of the virtual routing interface are blocked, the virtual routing interface can still route as long as at least one port in the protocol-based VLAN is not blocked by STP.

RSTP

Rapid Spanning Tree Protocol (RSTP) provides rapid traffic reconvergence for point-to-point links within a few milliseconds (less than 500 milliseconds) following the failure of a bridge or bridge port. This reconvergence occurs more rapidly than that provided by STP because convergence in RSTP bridges is based on the explicit handshakes between designated ports and their connected root ports rather than on timer values.

MSTP

With Multiple Spanning Tree Protocol (MSTP), the entire network runs a common instance of RSTP. Within the common instance, one or more VLANs can be individually configured into distinct regions. The entire network runs the Common Spanning Tree (CST) instance and the regions run a local instance, or Internal Spanning Tree (IST). Because the CST treats each IST as a single bridge,

ports are blocked to prevent loops that might occur within an IST and also throughout the CST. In addition, MSTP can co-exist with individual devices running STP or RSTP in the Common and Internal Spanning Tree instance (CIST). With the exception of the provisions for multiple instances, MSTP operates exactly like RSTP.

STP show commands

show spanning-tree

Syntax: show spanning-tree [**brief** | **ethernet** *unit/port* | **port-channel** *channel-id*| **stp-enabled-only**]

- **brief** - Shows a brief summary of STP settings for each port.
- **ethernet** *unit/port* - Specifies a port within the VLAN for detailed STP information.
- **port-channel** *channel-id* - Specifies a trunk within the VLAN for detailed STP information.
- **stp-enabled-only** - Shows STP settings for the switch and for STP-enabled ports.

This command displays global settings for STP.

```
Console# show spanning-tree
Spanning Tree Information
---------------------------------------------------------------
 Spanning Tree Mode              : STP
 Spanning Tree Enabled/Disabled  : Enabled
 Instance                        : 0
 VLANs Configured                : 1-4093
 Priority                        : 32768
 Bridge Hello Time (sec.)        : 2
 Bridge Max. Age (sec.)          : 20
 Bridge Forward Delay (sec.)     : 15
 Root Hello Time (sec.)          : 2
 Root Max. Age (sec.)            : 20
 Root Forward Delay (sec.)       : 15
 Max. Hops                       : 20
 Remaining Hops                  : 20
 Designated Root                 : 32768.0001ECF8D8C6
 Current Root Port               : 1
 Current Root Cost               : 100000
 Number of Topology Changes      : 2
 Last Topology Change Time (sec.): 790
 Transmission Limit              : 3
 Path Cost Method                : Long
 Flooding Behavior               : To VLAN
 Cisco Prestandard               : Disabled
```

This command displays detailed STP information (in this instance, for Port 1).

```
Console# show spanning-tree ethernet 1/1
Eth 1/ 1 Information
---------------------------------------------------------------
 Admin Status                     : Enabled
 Role                             : Root
 State                            : Forwarding
 Admin Path Cost                  : 0
 Oper Path Cost                   : 100000
 Priority                         : 128
 Designated Cost                  : 0
```

```
 Designated Port                  : 128.16
 Designated Root                  : 32768.0001ECF8D8C6
 Designated Bridge                : 32768.0001ECF8D8C6
 Forward Transitions              : 2
 Admin Edge Port                  : Auto
 Oper Edge Port                   : Disabled
 Admin Link Type                  : Auto
 Oper Link Type                   : Point-to-point
 Flooding Behavior                : Enabled
 Spanning-Tree Status             : Enabled
 Loopback Detection Status        : Enabled
 Loopback Detection Release Mode  : Auto
 Loopback Detection Trap          : Disabled
 Loopback Detection Action        : Block
 Root Guard Status                : Disabled
 BPDU Guard Status                : Disabled
 BPDU Guard Auto Recovery         : Disabled
 BPDU Guard Auto Recovery Interval : 300
 BPDU Filter Status               : Disabled
```

This command displays global settings for RSTP.

```
Console# show spanning-tree
Spanning Tree Information
---------------------------------------------------------------
 Spanning Tree Mode               : RSTP
 Spanning Tree Enabled/Disabled   : Enabled
 Instance                         : 0
 VLANs Configured                 : 1-4093
 Priority                         : 32768
 Bridge Hello Time (sec.)         : 2
 Bridge Max. Age (sec.)           : 20
 Bridge Forward Delay (sec.)      : 15
 Root Hello Time (sec.)           : 2
 Root Max. Age (sec.)             : 20
 Root Forward Delay (sec.)        : 15
 Max. Hops                        : 20
 Remaining Hops                   : 20
 Designated Root                  : 32768.00E00C109000
 Current Root Port(Eth)           : 1/1
 Current Root Cost                : 100000
 Number of Topology Changes       : 1
 Last Topology Change Time (sec.): 494
 Transmission Limit               : 3
 Path Cost Method                 : Long
 Flooding Behavior                : To VLAN
 Cisco Prestandard                : Disabled
---------------------------------------------------------------
Eth 1/ 1 Information
---------------------------------------------------------------
 Admin Status                     : Enabled
 Role                             : Root
 State                            : Forwarding
 Admin Path Cost                  : 0
 Oper Path Cost                   : 100000
 Priority                         : 128
 Designated Cost                  : 0
 Designated Port                  : 128.9
 Designated Root                  : 32768.00E00C109000
 Designated Bridge                : 32768.00E00C109000
```

```
 Forward Transitions               : 2
 Admin Edge Port                   : Auto
 Oper Edge Port                    : Disabled
 Admin Link Type                   : Auto
 Oper Link Type                    : Point-to-point
 Flooding Behavior                 : Enabled
 Spanning-Tree Status              : Enabled
 Loopback Detection Status         : Enabled
 Loopback Detection Release Mode   : Auto
 Loopback Detection Trap           : Disabled
 Loopback Detection Action         : Block
 Root Guard Status                 : Disabled
 BPDU Guard Status                 : Disabled
 BPDU Guard Auto Recovery          : Disabled
 BPDU Guard Auto Recovery Interval : 300
 BPDU Filter Status                : Disabled
...
```

This command displays global settings for MSTP.

```
Console# show spanning-tree
Spanning Tree Information
---------------------------------------------------------------
 Spanning Tree Mode              : MSTP
 Spanning Tree Enabled/Disabled  : Enabled
 Instance                        : 0
 VLANs Configured                : 1-4093
 Priority                        : 32768
 Bridge Hello Time (sec.)        : 2
 Bridge Max. Age (sec.)          : 20
 Bridge Forward Delay (sec.)     : 15
 Root Hello Time (sec.)          : 2
 Root Max. Age (sec.)            : 20
 Root Forward Delay (sec.)       : 15
 Max. Hops                       : 20
 Remaining Hops                  : 20
 Designated Root                 : 32768.0.00E00C109000
 Current Root Port(Eth)          : 1/1
 Current Root Cost               : 100000
 Number of Topology Changes      : 2
 Last Topology Change Time (sec.): 46
 Transmission Limit              : 3
 Path Cost Method                : Long
 Flooding Behavior               : To VLAN
 Cisco Prestandard               : Disabled
---------------------------------------------------------------
Eth 1/ 1 Information
---------------------------------------------------------------
 Admin Status                    : Enabled
 Role                            : Root
 State                           : Forwarding
 External Admin Path Cost        : 0
 Internal Admin Path Cost        : 0
 External Oper Path Cost         : 100000
 Internal Oper Path Cost         : 100000
 Priority                        : 128
 Designated Cost                 : 0
 Designated Port                 : 128.9
 Designated Root                 : 32768.0.00E00C109000
 Designated Bridge               : 32768.0.00E00C109000
```

```
 Forward Transitions               : 3
 Admin Edge Port                   : Auto
 Oper Edge Port                    : Disabled
 Admin Link Type                   : Auto
 Oper Link Type                    : Point-to-point
 Flooding Behavior                 : Enabled
 Spanning-Tree Status              : Enabled
 Loopback Detection Status         : Enabled
 Loopback Detection Release Mode   : Auto
 Loopback Detection Trap           : Disabled
 Loopback Detection Action         : Block
 Root Guard Status                 : Disabled
 BPDU Guard Status                 : Disabled
 BPDU Guard Auto Recovery          : Disabled
 BPDU Guard Auto Recovery Interval : 300
 BPDU Filter Status                : Disabled
...
```

Configuration notes

- Changing the STP state of the primary port in a trunk group affects all ports in the trunk group.
- With RSTP, rapid convergence will not occur on ports connected to shared media devices, such as hubs. To take advantage of the rapid convergence provided by RSTP, make sure to explicitly configure all point-to-point links in a topology.

  This command shows how to explicitly configure an interface which is attached to a LAN segment at the end of a bridged LAN or to an end node.

  ```
  Console(config)# interface ethernet 1/5
  Console(config-if)# spanning-tree edge-port
  Console(config-if)#
  ```

Common diagnostic scenarios

- Spanning Tree loops.
- Spanning Tree reacts to topology changes and port flapping.
- Port flapping can trigger a new Spanning Tree learning process.

LACP trunking

The Link Aggregation Control Protocol (LACP) allows ports on both sides of a redundant link to automatically configure themselves into a trunk link (aggregate link), eliminating the need for manual configuration. LACP has two modes:

- Active mode – When active link aggregation is enabled, the Brocade port can exchange standard LACP Data Unit (LACPDU) messages to negotiate trunk group configuration with the port on the other side of the link. In addition, the Brocade port actively sends LACPDU messages on the link to search for a link aggregation partner at the other end of the link, and can initiate an LACPDU exchange to negotiate link aggregation parameters with an appropriately configured remote port.

- Passive mode – In passive link aggregation, the Brocade port can exchange LACPDU messages with the port at the remote end of the link, but this port cannot search for a link aggregation port or initiate negotiation of an aggregate link. In passive mode, the port at the remote end of the link must initiate the LACPDU exchange.

When you enable link aggregation on a group of Brocade ports, the Brocade ports can negotiate with the ports at the remote ends of the links to establish trunk groups.

Trunk show commands

The following show commands display information about trunking configurations.

show lacp internal

Syntax: show lacp [*port-channel*] **internal**

port-channel - Local identifier for a link aggregation group. (Range: 1-5)

This command displays trunk information for configuration settings and the operational state for the local side.

```
Console# show lacp 1 internal
Port Channel : 1
------------------------------------------------------------------------
Oper Key  : 3
Admin Key : 0
Eth 1/ 1
------------------------------------------------------------------------
  LACPDUs Internal     : 30 seconds
  LACP System Priority : 32768
  LACP Port Priority   : 32768
  Admin Key            : 3
  Oper Key             : 3
  Admin State          : defaulted, aggregation, long timeout, LACP-activity
  Oper State           : distributing, collecting, synchronization,
                         aggregation, long timeout, LACP-activity
.
.
.
```

show lacp neighbors

Syntax: show lacp [*port-channel*] **internal**

port-channel - Local identifier for a link aggregation group. (Range: 1-5)

This command displays trunk information for configuration settings and the operational state for the remote side.

```
Console# show lacp 1 neighbors
Port Channel 1 neighbors
------------------------------------------------------------------------
Eth 1/ 1
------------------------------------------------------------------------
  Partner Admin System ID   : 32768, 00-00-00-00-00-00
  Partner Oper System ID    : 32768, 00-12-CF-61-24-2F
  Partner Admin Port Number : 1
  Partner Oper Port Number  : 1
  Port Admin Priority       : 32768
  Port Oper Priority        : 32768
  Admin Key                 : 0
  Oper Key                  : 3
```

```
  Admin State:              defaulted, distributing, collecting,
                            synchronization, long timeout,
  Oper State:               distributing, collecting, synchronization,
                            aggregation, long timeout, LACP-activity
.
.
.
```

Configuration notes

- You cannot use 802.3ad link aggregation on a port configured as a member of a static trunk group.
- When LACP dynamically adds or changes a trunk group, the **show interface status port-channel** command displays the trunk as both configured and active. However, the **show running-config** commands do not contain a trunk command defining the new or changed trunk group.
- You can enable link aggregation on 802.1q tagged ports that belong to more than one port-based VLAN.
- Brocade recommends that you disable or remove the cables from the ports you plan to enable for dynamic link aggregation. Doing so prevents the possibility that LACP will use a partial configuration to talk to the other side of a link. A partial configuration does not cause errors, but sometimes requires LACP to be disabled and re-enabled on both sides of the link to ensure that a full configuration is used. It is easier to disable a port or remove its cable first. This applies both for active link aggregation and passive link aggregation.

Trunk formation rules

When troubleshooting trunks, make sure the following rules for trunk formation have been considered:

- Any number of ports between 2 and 12 within the same chassis can be used to configure a trunk port.
- Ports in a trunk must have the same speed, negotiation mode, and Quality of Service (QoS) priority or the trunk is rejected.
- All ports configured in a trunk must be configured with the same port attributes.
- Primary port policy applies to all secondary ports. No trunk is rejected.
- The trunk is rejected if any trunk port has mirroring or monitoring configured.
- The trunk is rejected if any trunk port has VLAN or inner-VLAN translation configured (also known as VLAN trunking).

Common diagnostic scenarios

- LACP trunk links may not operate properly between Brocade devices and third-party devices because of a mismatch between the link configurations. If the link is fixed on the third-party side, the link on the Brocade side must be a trunk. If it is link-aggregated on the third-party side, then it must be the same on the Brocade side.
- LACP links may not operate properly due to misconfigurations. Contact Brocade Technical Support for help with configuration issues.

VLAN trunking

VLAN trunking allows traffic from one VLAN to be transported across a different VLAN. Packets with unknown VLAN IDs entering the switch at the ingress port are allowed to pass through to any configured VLAN trunking port. When unknown VLAN traffic must pass through one or more intermediate switches to reach its destination, you can configure VLAN flooding on ports that form a path across the intermediate switches to connect the source of this traffic to its destination.

This feature is useful for service providers who must carry traffic from different customers across their network while preserving the VLAN ID and priority information of the customer network.

VLAN trunking show commands

show interfaces status

Syntax: show interfaces status ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

This command displays the configuration status of VLAN trunking for the specified port.

```
Console# show interfaces status ethernet 1/1
Information of Eth 1/1
 Basic Information:
  Port Type              : 1000T
  MAC Address            : 70-72-CF-32-DD-FE
 Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm        : Enabled
  Broadcast Storm Limit  : 64 Kbits/second
  Multicast Storm        : Disabled
  Multicast Storm Limit  : 64 Kbits/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 64 Kbits/second
  Flow Control           : Disabled
  VLAN Trunking          : Enabled
  LACP                   : Disabled
  Port Security          : Disabled
  Max MAC Count          : 0
  Port Security Action   : None
  Media Type             : SFP preferred auto
 Current Status:
  Link Status            : Up
  Port Operation Status  : Up
  Operation Speed-duplex : 100full
  Up Time                : 0w 0d 0h 40m 36s (2436 seconds)
  Flow Control Type      : None
```

Ethernet Ring Protection switching

The ITU G.8032 recommendation specifies a protection switching mechanism and protocol for Ethernet layer network rings. Ethernet rings can provide wide-area multipoint connectivity and redundancy more economically due to their reduced number of links. The mechanisms and protocol defined in G.8032 achieve highly reliable and stable protection; and never form loops, which would fatally affect network operation and service availability.

To configure Ethernet Protection Ring Switching (ERPS), follow the guidelines in the *Brocade 6910 Ethernet Access Switch Configuration Guide*. If you encounter any problems, use the following show command to display a summary of the configuration settings and operational status for all rings, or detailed information for a specific ring.

ERPS show commands

Syntax: show erps

Syntax: **show erps** [**domain** *ring-name*]

ring-name - Name of a specific ERPS ring. (Range: 1-32 characters)

This command displays the configuration settings and operational status of ERPS.

```
Console# show erps
ERPS Status : Enabled
Number of ERPS Domains : 1
Domain State MEL Enabled West East RPL Owner Ctrl VLAN
------------ ---------- --- ------- -------- -------- --------- ---------
rd1 Idle 0 Yes Eth 1/12 Eth 1/10 Yes 100
rd2 Protection 0 Yes Eth 1/3 Eth 1/4 No 200
```

This command displays detailed information for a specific ring.

```
Console#show erps domain rd1
Domain Name : rd1
Admin Status : Enabled
MEG Level : 1
Node ID : 00-12-CF-61-24-2F
Node State : Idle
West Port : Eth 1/ 1 (Blocking)
East Port : Eth 1/ 2 (Forwarding)
RPL Port : West
RPL Owner : Enabled
Holdoff Timer : 300 ms
Guard Timer : 300 ms
WTR Timer : 5 minutes
Control VLAN : 2
Propagate TC : Disabled
```

Connectivity Fault Management

Connectivity Fault Management (CFM) is an OAM protocol that includes proactive connectivity monitoring using continuity check messages, fault verification through loop back messages, and fault isolation by examining end-to-end connections between provider edge devices or between customer edge devices.

CFM is implemented as a service level protocol based on service instances which encompass only that portion of the metropolitan area network supporting a specific customer. CFM can also provide controlled management access to a hierarchy of maintenance domains (such as the customer, service provider, and equipment operator).

This switch supports functions for defining the CFM structure, including domains, maintenance associations, and maintenance access points. It also supports fault detection through continuity check messages for all known maintenance points, and cross-check messages which are used to verify a static list of remote maintenance points located on other devices (in the same maintenance association) against those found through continuity check messages. Fault verification is supported using loop back messages, and fault isolation with link trace messages. Fault notification is also provided by SNMP alarms which are automatically generated by maintenance points when connectivity faults or configuration errors are detected in the local maintenance domain.

To configure CFM), follow the guidelines in the *Brocade 6910 Ethernet Access Switch Configuration Guide*. If you encounter any problems, use the following show command to display a summary of the configuration settings and operational status for all rings, or detailed information for a specific ring.

CFM show commands

This commands displays CFM configuration settings, including global settings, SNMP traps, and interface settings.

show ethernet cfm configuration

Syntax: show ethernet cfm configuration {**global** | **traps** | **interface** *interface*}

global – Displays global settings including CFM global status, cross-check start delay, and link trace parameters.

traps – Displays the status of all continuity check and cross-check traps.

interface – Displays CFM status for the specified interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

port-channel *channel-id* (Range: 1-12)

This example shows the global settings for CFM.

```
Console# show ethernet cfm configuration global
CFM Global Status         : Enabled
Crosscheck Start Delay    : 10 seconds
Linktrace Cache Status    : Enabled
Linktrace Cache Hold Time : 100 minutes
Linktrace Cache Size      : 100 entries
```

This example shows the configuration status for continuity check and cross-check traps.

```
Console# show ethernet cfm configuration traps
CC MEP Up Trap                : Disabled
CC MEP Down Trap              : Disabled
CC Configure Trap             : Disabled
CC Loop Trap                  : Disabled
Cross Check MEP Unknown Trap  : Disabled
```

```
Cross Check MEP Missing Trap  : Disabled
Cross Check MA Up             : Disabled
```

This example shows the CFM status for port 1.

```
Console #show ethernet cfm configuration interface ethernet 1/1
Ethernet 1/1 CFM Status:Enabled
```

This command displays configured maintenance domains.

show ethernet cfm md

Syntax: show ethernet cfm md [**level** *level*]

level – Maintenance level. (Range: 0-7)

This example shows all configured maintenance domains.

```
Console#show ethernet cfm md
MD Index  MD Name               Level  MIP Creation  Archive Hold Time (m.)
--------  --------------------  -----  ------------  ----------------------
       1  rd                        0  default                          100
```

This command displays configured maintenance associations.

show ethernet cfm ma

Syntax: show ethernet cfm ma [**level** *level*]

level – Maintenance level. (Range: 0-7)

This example shows all configured maintenance associations.

```
Console# show ethernet cfm ma
MD Name         MA Index MA Name         Primary VID  CC Interval MIP Creation
--------------- -------- --------------- ----------- ----------- ------------
steve                  1 voip                      1           4 Default
```

This command displays maintenance points configured on this device.

show ethernet cfm maintenance-points local

Syntax: show ethernet cfm maintenance-points local
{**mep** [**domain** *domain-name* | **interface** *interface* | **level** *level-id*] |
mip [**domain** *domain-name* | **level** *level-id*]}

mep – Displays only local maintenance end points.

mip – Displays only local maintenance intermediate points.

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

interface – Displays CFM status for the specified interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

port-channel *channel-id* (Range: 1-12)

level-id – Maintenance level for this domain. (Range: 0-7)

This example shows all MEPs configured on this device for maintenance domain rd.

```
Console#show ethernet cfm maintenance-points local mep
MPID MD Name          Level Direct VLAN Port     CC Status MAC Address
---- ---------------- ----- ------ ---- -------- --------- -----------------
   1 rd                   0 UP        1 Eth 1/ 1 Enabled   00-12-CF-3A-A8-C0
```

This command displays detailed CFM information about a specified local MEP in the continuity check database.

show ethernet cfm maintenance-points local detail mep

Syntax: show ethernet cfm maintenance-points local detail mep [**domain** *domain-name* | **interface** *interface* | **level** *level-id*]

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

interface – Displays CFM status for the specified interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

port-channel *channel-id* (Range: 1-12)

level-id – Maintenance level for this domain. (Range: 0-7)

This example shows detailed information about the local MEP on port 1.

```
Console# show ethernet cfm maintenance-points local detail mep interface ethernet
  1/1
MEP Settings:
-------------
MPID                  : 1
MD Name               : vopu
MA Name               : r&d
MA Name Format        : Character String
Level                 : 0
Direction             : Up
Interface             : Eth 1/ 1
CC Status             : Enabled
MAC Address           : 00-E0-0C-00-00-FD
Defect Condition      : No Defect
Received RDI          : False
AIS Status            : Enabled
AIS Period            : 1 seconds
AIS Transmit Level    : Default
Suppress Alarm        : Disabled
Suppressing Alarms    : Disabled
```

This command displays detailed CFM information about a specified remote MEP in the continuity check database.

show ethernet cfm maintenance-points remote detail

Syntax: show ethernet cfm maintenance-points remote detail
{**mac** *mac-address* | **mpid** *mpid*}
[**domain** *domain-name* | **level** *level-id* | **ma** *ma-name*]

mac-address – MAC address of a remote maintenance point.
This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

mpid – Maintenance end point identifier. (Range: 1-8191)

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

level-id – Authorized maintenance level for this domain. (Range: 0-7)

ma-name – Maintenance association name. (Range: 1-45 alphanumeric characters)

This example shows detailed information about the remote MEP designated by MPID 2.

```
Console# show ethernet cfm maintenance-points remote detail mpid 2
MAC Address            : 00-0D-54-FC-A2-73
Domain/Level           : voip / 3
MA Name                : rd
Primary VLAN           : 1
MPID                   : 2
CC Lifetime            : 645 seconds
Age of Last CC Message : 2 seconds
Frame Loss             : 137
CC Packet Statistics   : 647/1
Port State             : Up
Interface State        : Up
Crosscheck Status      : Enabled
```

This command displays CFM continuity check errors logged on this device.

show ethernet cfm errors

Syntax: show ethernet cfm errors [**domain** *domain-name* | **level** *level-id*]

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

level-id – Authorized maintenance level for this domain. (Range: 0-7)

This example shows a continuity check error logged for this device.

```
Console# show ethernet cfm errors
Level VLAN MPID Interface Remote MAC        Reason           MA Name
----- ---- ---- --------- ----------------- ---------------- ----------------
5      2     40 Eth 1/1   ab.2f.9c.00.05.01 LEAK             provider_1_2
```

This command displays information about remote maintenance points configured statically in a cross-check list.

show ethernet cfm maintenance-points remote crosscheck

Syntax: show ethernet cfm maintenance-points remote crosscheck [**domain** *domain-name* | **mpid** *mpid*]

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

mpid – Maintenance end point identifier. (Range: 1-8191)

This example shows all remote MEPs statically configured on this device.

```
Console# show ethernet cfm maintenance-points remote crosscheck
MPID  MA Name               Level  VLAN  MEP Up  Remote MAC Address
----  --------------------  -----  ----  ------  ------------------
   2  downtown                  4     2  Yes     00-0D-54-FC-A2-73
```

This command displays the contents of the link trace cache.

show ethernet cfm linktrace-cache

Syntax: show ethernet cfm linktrace-cache

This example shows the contents of the link trace cache.

```
Console# show ethernet cfm linktrace-cache
Hops MA             IP / Alias              Ingress MAC       Ing. Action Relay
                    Forwarded               Egress MAC        Egr. Action
---- -------------- ----------------------- ----------------- ----------- -----
   2 rd             192.168.0.6             00-12-CF-12-12-2D ingOk       Hit
                    Not Forwarded
```

Operation, Administration and Maintenance

The switch provides OAM (Operation, Administration and Maintenance) remote management tools required to monitor and maintain the links to subscriber CPEs (Customer Premise Equipment). OAM can be used to perform loopback testing, or to display remote device information.

OAM show commands

This command displays counters for various OAM PDU message types.

show efm oam counters interface

Syntax: show efm oam counters interface [*interface-list*]

interface-list - unit/port

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-12)

This example displays counters for OAM PDU message types.

```
Console# show efm oam counters interface 1/1
Port OAMPDU Type           TX         RX
---- -------------------- ---------- ----------
1/1  Information          1121       1444
1/1  Event Notification   0          0
1/1  Loopback Control     1          0
1/1  Organization Specific 76        0
```

This command displays the OAM event log for the specified port(s) or for all ports that have logs.

show efm oam event-log interface

Syntax: show efm oam event-log interface [*interface-list*]

interface-list - unit/port

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-12)

This example displays the OAM event log.

```
Console# show efm oam event-log interface 1/1
OAM event log of Eth 1/1:
 00:24:07 2001/01/01
 "Unit 1, Port 1: Dying Gasp at Remote"
```

This command displays the results of an OAM remote loopback test.

show efm oam remote-loopback interface

Syntax: show efm oam remote-loopback interface [*interface-list*]

interface-list - unit/port

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-12)

This example displays the results of an OAM remote loopback test.

```
Console# show efm oam remote-loopback interface 1/1
Port OAM loopback Tx OAM loopback Rx Loss Rate
---- --------------- --------------- ---------
1/1            10000            9999    0.01 %
```

This command displays OAM configuration settings and event counters.

show efm oam status interface

Syntax: show efm oam status interface [*interface-list*] [**brief**]

interface-list - unit/port

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-12)

brief - Displays a brief list of OAM configuration states.

This example displays a full list of OAM configuration settings and event counters.

```
Console# show efm oam status interface 1/1
OAM information of Eth 1/1:
 Basic Information:
  Admin State                    : Enabled
  Operation State                : Operational
  Mode                           : Active
  Remote Loopback                : Disabled
  Remote Loopback Status         : No loopback
  Dying Gasp                     : Enabled
  Critical Event                 : Enabled
  Link Monitor (Errored Frame)   : Enabled
 Link Monitor:
  Errored Frame Window (100msec) : 10
  Errored Frame Threshold        : 1
```

This example displays a summary of OAM configuration settings and event counters.

```
Console#s how efm oam status interface 1/1 brief
$ = local OAM in loopback
* = remote OAM in loopback

Port Admin   Mode    Remote   Dying   Critical Errored
     State           Loopback Gasp    Event    Frame
---- ------- ------- -------- ------- -------- -------
1/1  Enabled Active  Disabled Enabled Enabled  Enabled
```

This command displays information about attached OAM-enabled devices.

show efm oam status remote interface

Syntax: show efm oam status remote interface [*interface-list*]

interface-list - unit/port

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-12)

This example displays information about attached OAM-enabled devices.

```
Console#show efm oam status remote interface 1/1
Port MAC Address       OUI    Remote   Unidirectional Link    MIB Variable
                              Loopback               Monitor Retrieval
---- ----------------- ------ -------- -------------- ------- ------------
1/1  00-12-CF-6A-07-F6 000084 Enabled  Disabled       Enabled Disabled
```

Chapter

ACL and QoS Diagnostics 5

This chapter provides diagnostic information for Access Control List (ACL) and Quality of Service (QoS) environments, including traffic management.

ACLs

Access Control List (ACL) show commands help users to diagnose and determine the cause of faults for ACL-related features. For details on Layer 2 ACLs, refer to the Layer 2 ACL chapter in the *Brocade BR6910 Configuration Guide*.

ACL show commands

show access-list

Syntax: **show ip** {**standard** | **extended**} **access-list** [*acl-name*]
show ipv6 {**standard** | **extended**} **access-list** [*acl-name*]
show mac ace ss-list [*acl-name*]

This command displays the ACLs configured on a Brocade device.

Enter the ACL name for the *acl-name* parameter to display a specific ACL, enter this command without a name to display all configured ACLs for the specified ACL type, or enter the command without specifying the ACL type or name to display all configured ACLs.

For a specific ACL, enter a command similar to the following example.

```
Console# show ip standard access-list david
IP standard access-list david:
 permit host 10.1.1.21
 permit 168.92.0.0 255.255.15.0
```

Common diagnostic scenarios

- When an ACL was removed from a port with port mapping (ACL-based rate-limiting) configured, the Brocade 6910 stopped all traffic on this port.

  If you make an ACL configuration change, you must reapply the ACLs to their interfaces for the change to take effect. An ACL configuration change includes any of the following actions:

  - Adding, changing, or removing an ACL or an entry in an ACL
  - Changing ToS-based QoS mappings

  To reapply an ACL following an ACL configuration change, enter the **ip access-group** command at the interface configuration level of the CLI as shown in the following example.

  ```
  Console(config)# interface ethernet 1/2
  Console(config-if)# ip access-group david in
  ```

QoS

Quality of Service (QoS) features prioritize the use of bandwidth in a switch. When QoS features are enabled, traffic is classified as it arrives at the switch, and processed on the basis of configured priorities. Traffic can be dropped, prioritized for delivery, or subjected to limited delivery options, depending on how you configure QoS features.

QoS show commands

show qos map trust-mode

Syntax: show qos map trust-mode interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

port-channel *channel-id* (Range: 1-12)

This command displays the QoS mapping mode.

```
Console# show qos map trust-mode interface ethernet 1/5
Information of Eth 1/5
COS Map mode: CoS mode
```

show qos map cos-dscp

Syntax: show qos map cos-dscp interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

port-channel *channel-id* (Range: 1-12)

If a packet arrives with a 802.1Q header but it is not an IP packet, then this table is used to map the Class of Service/Canonical Format Indicator (CoS/CFI) values in the ingress packet to priority and drop precedence values for internal processing

This command shows the ingress CoS/CFI to internal Differentiated Services Code Point Service (DSCP) map.

```
Console# show qos map cos-dscp interface ethernet 1/5
CoS Information of Eth 1/5
CoS-DSCP map.(x,y),x: PHB,y: drop precedence:
CoS : CFI 0 1
---------------------------------
0 (0,0) (0,0)
1 (1,0) (1,0)
2 (2,0) (2,0)
3 (3,0) (3,0)
4 (4,0) (4,0)
5 (5,0) (5,0)
6 (6,0) (6,0)
7 (7,0) (7,0)
```

show qos map dscp-mutation

Syntax: show qos map cos-dscp interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

port-channel *channel-id* (Range: 1-12)

This map is only used when the QoS mapping mode is set to “DSCP” by the **qos map trust-mode** command, and the ingress packet type is IPv4.

Two QoS domains can have different DSCP definitions, so the DSCP-to-PHB/Drop Precedence mutation map can be used to modify one set of DSCP values to match the definition of another domain. The mutation map should be applied at the receiving port (ingress mutation) at the boundary of a QoS administrative domain.

This command shows the ingress DSCP to internal DSCP mutation map.

```
Console# show qos map dscp-mutation interface ethernet 1/5
Information of Eth 1/5
 DSCP mutation map.(x,y),x: PHB,y: drop precedence:
 d1: d2 0     1     2     3     4     5     6     7     8     9
 ------------------------------------------------------------------------
 0 :    (0,0) (0,1) (0,0) (0,3) (0,0) (0,1) (0,0) (0,3) (1,0) (1,1)
 1 :    (1,0) (1,3) (1,0) (1,1) (1,0) (1,3) (2,0) (2,1) (2,0) (2,3)
 2 :    (2,0) (2,1) (2,0) (2,3) (3,0) (3,1) (3,0) (3,3) (3,0) (3,1)
 3 :    (3,0) (3,3) (4,0) (4,1) (4,0) (4,3) (4,0) (4,1) (4,0) (4,3)
 4 :    (5,0) (5,1) (5,0) (5,3) (5,0) (5,1) (5,0) (5,3) (6,0) (6,1)
 5 :    (6,0) (6,3) (6,0) (6,1) (6,0) (6,3) (7,0) (7,1) (7,0) (7,3)
 6 :    (7,0) (7,1) (7,0) (7,3)
```

show qos map phb-queue

Syntax: show qos map phb-queue interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

port-channel *channel-id* (Range: 1-12)

This command shows the internal per-hop behavior to hardware queue map.

```
Console# show qos map phb-queue interface ethernet 1/5
Information of Eth 1/5
 PHB-queue map:
 PHB:       0     1     2     3     4     5     6     7
 ---------------------------------------------------------
 queue:     2     0     1     3      4     5     6     7
```

show queue mode

Syntax: show queue mode

This command shows the current queue mode.

```
Console# show queue mode

Queue Mode : Weighted Round Robin Mode
```

show queue weight

Syntax: show queue weight

This command displays the weights used for the weighted queues.

```
Console# show queue weight
 Queue ID  Weight
 --------  ------
        0       1
        1       2
        2       4
        3       6
        4       8
        5      10
        6      12
        7      14
```

Chapter

Security Diagnostics

6

This chapter describes diagnostic information for security environments on the Brocade 6910 series switches.

802.1x

802.1x port security allows you to configure a Brocade device to grant access to a port based on information supplied by a client to an authentication server.

This section describes how to use show commands to monitor 802.1x configurations and activity on Brocade 6910 series switches.

802.1x show commands

You can display the following 802.1x-related information:

- Information about the 802.1x configuration on the device and on individual ports
- Statistics about the EAPOL frames passing through the device
- Information about the 802.1x multiple client configuration

show dot1x

Syntax: show dot1x

This command displays information about the 802.1x configuration, as shown in the following example.

```
Console# show dot1x
Global 802.1X Parameters
 System Auth Control      : Enabled

Authenticator Parameters:
 EAPOL Pass Through       : Disabled

Supplicant Parameters:
Identity Profile Username : steve

802.1X Port Summary

Port     Type          Operation Mode Control Mode       Authorized
-------- ------------- -------------- ------------------ ----------
Eth 1/ 1 Disabled      Single-Host    Force-Authorized   Yes
Eth 1/ 2 Disabled      Single-Host    Force-Authorized   Yes
...
Eth 1/11 Disabled Single-Host Force-Authorized Yes
Eth 1/12 Enabled Single-Host Auto Yes
802.1X Port Details
802.1X Supplicant is disabled on port 1/1
...
```

```
802.1X Authenticator is enabled on port 12
Reauthentication     : Enabled
Reauth Period        : 3600
Quiet Period         : 60
TX Period            : 30
Supplicant Timeout   : 30
Server Timeout       : 10
Reauth Max Retries   : 2
Max Request          : 2
Operation Mode       : Multi-host
Port Control         : Auto
Intrusion Action     : Block traffic

Supplicant           : 00-e0-29-94-34-65

Authenticator PAE State Machine
 State               : Authenticated
 Reauth Count        : 0
 Current Identifier  : 3

 Backend State Machine
 State               : Idle
 Request Count       : 0
 Identifier(Server)  : 2

Reauthentication State Machine
State : Initialize
```

show dot1x interface

Syntax: show dot1x interface ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

This command displays information about the 802.1x configuration on a specified port, as shown in the following example.

```
Console# show dot1x interface ethernet 1/12

802.1X Authenticator is enabled on port 1/12
 Reauthentication     : Disabled
 Reauth Period        : 3600 seconds
 Quiet Period         : 60 seconds
 TX Period            : 30 seconds
 Supplicant Timeout   : 30 seconds
 Server Timeout       : 10 seconds
 Reauth Max Retries   : 2
 Max Request          : 2
 Operation Mode       : Single-Host
 Port Control         : Auto
 Intrusion Action     : Block traffic

Supplicant            : 00-00-00-00-00-00

 Authenticator PAE State Machine
  State               : Initialize
  Reauth Count        : 0
  Current Identifier  : 0
```

```
 Backend State Machine
  State               : Initialize
  Request Count       : 0
  Identifier (Server) : 0

 Reauthentication State Machine
  State               : Initialize
```

show dot1x statistics

Syntax: show dot1x statistics interface ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

This command displays 802.1x statistics for a specified port, as shown in the following example.

```
Console# show dot1x statistics interface ethernet 1/12

Eth 1/12
Rx: EAPOL      EAPOL      EAPOL      EAPOL      EAP      EAP      EAP
    Start      Logoff     Invalid    Total    Resp/ID  Resp/Oth LenError
        0          0          0          0        0        0        0

    Last      Last
EAPOLVer     EAPOLSrc
       0     00-00-00-00-00-00

Tx: EAPOL      EAP      EAP
    Total     Req/ID   Req/Oth
        0         0        0
802.1X Supplicant is disabled on port 1/12
```

Configuration notes

- The client's 802.1x MAC session establishes a relationship between the user name and the MAC address used for authentication. If a user attempts to gain access from different clients (with different MAC addresses), the user must be authenticated from each client.
- If a client has been denied access to the network (that is, the client's 802.1x MAC session is set to "access-denied"), then you can cause the client to be re-authenticated by manually disconnecting the client from the network, or by using the **dot1x re-authentication** command.
- When a client has been denied access to the network, the 802.1x MAC session is aged out if no traffic is received from the client's MAC address over a fixed hardware aging period (300 seconds). You can optionally change the software aging period for 802.1x MAC sessions or disable aging altogether. After the denied client's 802.1x MAC session is aged out, traffic from that client is no longer blocked, and the client can be re-authenticated.
- To implement 802.1x port security, at least one of the RADIUS servers identified to the Brocade device must support the 802.1x standard.

Port loop detection

Brocade port loop detection allows the Brocade device to detect loops and disable a port that is on the receiving end of a loop. A loop is detected by sending test packet BPDUs.

Port loop detection show commands

show spanning-tree

Syntax: show spanning-tree [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

port-channel *channel-id* (Range: 1-12)

This command displays the loop detection configuration, as shown in the following example.

```
Console# show spanning-tree ethernet 1/1
Eth 1/ 1 Information
------------------------------------------------------------
 Admin Status                      : Enabled
 Role                              : Root
 State                             : Forwarding
 Admin Path Cost                   : 0
 Oper Path Cost                    : 100000
 Priority                          : 128
 Designated Cost                   : 0
 Designated Port                   : 128.16
 Designated Root                   : 32768.0001ECF8D8C6
 Designated Bridge                 : 32768.0001ECF8D8C6
 Forward Transitions               : 1
 Admin Edge Port                   : Auto
 Oper Edge Port                    : Disabled
 Admin Link Type                   : Auto
 Oper Link Type                    : Point-to-point
 Flooding Behavior                 : Enabled
 Spanning-Tree Status              : Enabled
 Loopback Detection Status         : Enabled
 Loopback Detection Release Mode   : Auto
 Loopback Detection Trap           : Disabled
 Loopback Detection Action         : Block
 Root Guard Status                 : Disabled
 BPDU Guard Status                 : Disabled
 BPDU Guard Auto Recovery          : Disabled
 BPDU Guard Auto Recovery Interval : 300
 BPDU Filter Status                : Disabled
```

Configuration notes

A port is disabled only if a packet is looped back to that same port. Loop detection must be configured on the physical port.

Port mirroring and monitoring

You can monitor the traffic on the Brocade ports by configuring another port to mirror the traffic on the ports you want to monitor. The port thus configured is called a mirror port. By attaching a protocol analyzer to the mirror port, you can observe the traffic on the monitored ports.

Port mirroring show commands

show port monitor

Syntax: show port monitor [*interface* | **vlan** *vlan-id* | **mac-address** *mac-address*]

interface - **ethernet** *unit/port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-12)

vlan-id - VLAN ID (Range: 1-4093)

mac-address - MAC address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

This command displays the configuration settings for inbound or outbound traffic that is being mirrored to each mirror port, as shown in the following example.

```
Console# show port monitor
Port Mirroring
-------------------------------------
 Destination Port (listen port): Eth1/ 2
 Source Port (monitored port)  : Eth1/ 1
 Mode                          :RX
```

RADIUS

You can use a Remote Authentication Dial In User Service (RADIUS) server to secure the following types of access to the Brocade devices:

- Telnet access
- SSH access
- Web management access
- Access to the Privileged Exec level and CONFIG level of the CLI

NOTE
The Brocade devices do not support RADIUS security for SNMP access.

RADIUS show commands

show radius-server

Syntax: show radius-server

This command displays information about all RADIUS servers configured on the device.

```
Console# show radius-server

Remote RADIUS Server Configuration:

Global Settings:
 Authentication Port Number : 1812
 Accounting Port Number     : 1813
 Retransmit Times           : 2
 Request Timeout            : 5

Server 1:
 Server IP Address          : 10.11.12.13
 Authentication Port Number : 1812
 Accounting Port Number     : 1813
 Retransmit Times           : 2
 Request Timeout            : 5

RADIUS Server Group:
Group Name                Member Index
------------------------- -------------
radius                    1
```

show users

Syntax: show users

This command displays the privilege level of all management interface users.

```
Console# show users
  User Name Accounts:
  User Name                       Privilege Public-Key
  ------------------------------- --------- ----------
  admin                                  15 None
  guest                                   0 None
  steve                                  15 RSA

 Online Users:
  Line    User Name                        Idle time (h:m:s) Remote IP addr
  ------- -------------------------------- ----------------- ---------------
*console admin                                      0:00:00
 SSH 0   admin                                      0:00:00 192.168.0.99

 Web Online Users:
  Line  User Name                       Idle time (h:m:s) Remote IP Addr
  ----- ------------------------------- ----------------- ---------------
  HTTP  admin                                   0:00:00 192.168.0.9
```

Configuration notes

- You must deploy at least one RADIUS server in your network to provide authentication services.
- Brocade devices support authentication using up to five RADIUS servers. The device tries to use the servers in the order you add them to the device's configuration. If one RADIUS server is not responding, the Brocade device tries the next one in the list.
- You can use the **authentication login** command to select a sequence of authentication methods for all types of access to a device (CLI through Telnet, CLI Exec and CLI Privileged Exec levels). Use the **authentication enable** command to specify the sequence of authentication methods to use when changing from Normal Exec command mode to Privileged Exec command mode with the **enable** command.
- RADIUS command authorization can be performed only for commands entered from Telnet or SSH sessions, or from the console. No authorization is performed for commands entered at the Web management interface or for SNMP management applications.

SNMP

The Simple Network Management Protocol (SNMP) forms part of the Internet Protocol (IP) suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices administration and management.

SNMP is enabled by default on Brocade devices. SNMP must be enabled in order to manage a Brocade device using SNMP management applications.

SNMP show commands

show snmp

Syntax: show snmp

This command displays both the read-only and read-write community strings.

To display the SNMP community string, enter the following command.

```
Console# show snmp

SNMP Agent : Enabled

SNMP Traps :
 Authentication : Enabled
 Link-up-down   : Enabled

SNMP Communities :
   1. public, and the access level is read-only
   2. private, and the access level is read/write

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
```

```
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP Logging: Disabled
```

show snmp engine-id

Syntax: show snmp engine-id

This command displays the engine ID of a switch, as shown in the following example.

```
Console# show snmp engine-id
Local SNMP Engine ID    : 80000103037072CF32DDFD0000
Local SNMP Engine Boots : 36
```

show snmp group

Syntax: show snmp group

This command displays the definition of all SNMP groups, as shown in the following example.

```
Console# show snmp group
Group Name     : public
Security Model : v1
Read View      : defaultview
Write View     : No writeview specified
Notify View    : No notifyview specified
Storage Type   : volatile
Row Status     : active

Group Name     : public
Security Model : v2c
Read View      : defaultview
Write View     : No writeview specified
Notify View    : No notifyview specified
Storage Type   : volatile
Row Status     : active

Group Name     : private
Security Model : v1
Read View      : defaultview
Write View     : defaultview
Notify View    : No notifyview specified
Storage Type   : volatile
Row Status     : active

Group Name     : private
Security Model : v2c
Read View      : defaultview
Write View     : defaultview
Notify View    : No notifyview specified
Storage Type   : volatile
Row Status     : active
```

show snmp user

Syntax: show snmp user

This command displays the definition of local and remote SNMP user accounts, as shown in the following example.

```
Console# show snmp user
EngineId: 800000ca030030f1df9ca00000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active
```

Configuration notes

- SNMP read-only or read-write community strings are always required for SNMP access to the device.
- SNMP access is enabled by default.
- If you do not enable Telnet access, you can access the CLI using a serial connection to the console port. If you do not enable SNMP access, you will not be able to use or SNMP management applications.
- For management access, you must configure authentication-method lists if you want the device to authenticate access using local user accounts or a RADIUS server. Otherwise, the device will authenticate using only the locally based password for the Administrator privilege level.

TACACS and TACACS+

Terminal Access Controller Access Control System Plus (TACACS+) is an enhancement to the TACACS security protocol. TACACS+ improves on TACACS by separating the functions of authentication, authorization, and accounting (AAA) and by encrypting all the traffic between the Brocade device and the TACACS+ server.

TACACS+ show commands

show tacacs-server

Syntax: show tacacs-server

This command displays information about all TACACS+ servers configured on the device.

```
Console# show tacacs-server
```

```
Remote TACACS+ Server Configuration:

Global Settings:
 Server Port Number : 49
 Retransmit Times   : 2
 Timeout            : 5

Server 1:
 Server IP Address  : 10.11.12.13
 Server Port Number : 49
 Retransmit Times   : 2
 Timeout            : 4

Tacacs Server Group:
Group Name                Member Index
------------------------- -------------
tacacs+                   1
```

show users

Syntax: show users

This command displays the privilege level of users of all management interfaces.

```
Console# show users
 User Name Accounts:
  User Name Privilege Public-Key
  --------- --------- ----------
      admin        15 None
      guest         0 None
      steve        15 RSA

 Online Users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
  0 console   admin              0:14:14
* 1   VTY 0   admin              0:00:00 192.168.1.19
  2   SSH 1   steve              0:00:06 192.168.1.19

Web Online Users:
 Line        Remote IP Addr User Name Idle time (h:m:s)
 ----------- -------------- --------- ------------------
 1      HTTP    192.168.1.19     admin            0:00:00
```

Configuration notes

- You must deploy at least one TACACS or TACACS+ server in your network to provide authentication services.
- The Brocade device supports authentication using one TACACS or TACACS+ server.
- You can use the **authentication login** command to select a sequence of authentication methods for each type of access to a device (CLI through Telnet, CLI Normal Exec and CLI Privileged Exec levels). Use the **authentication enable** command to specify the sequence of authentication methods to use when changing from Normal Exec command mode to Privileged Exec command mode with the **enable** command.
- TACACS+ provides for authentication, authorization, and accounting, but an implementation or configuration is not required to employ all three.

- If you erase a **tacacs-server host** command (by entering the **no** form of the command), make sure you also erase the **authentication login** commands that specify only TACACS or TACACS+ as an authentication method. Otherwise, when you exit from the CONFIG mode or from a Telnet session, the system continues to believe that TACACS or TACACS+ is enabled and you will not be able to access the system.
- TACACS+ command authorization can be performed only for commands entered from Telnet or SSH sessions, or from the console. No authorization is performed for commands entered at the Web management interface.

Telnet and SSH connections

The first time you log on to the console port, you must use a serial connection in order to assign an IP address to the port. Once an IP address is assigned, you can access the CLI through a local Telnet, SSH, or SNMP connection through the management port. When accessing the CLI through Telnet, you may be prompted for a password. By default, the password required is the one you enter for general access at initial setup.

NOTE
Telnet, Web, and SNMP servers are enabled by default, but can be disabled selectively. SSH is disabled by default.

Telnet and SSH show commands

show ip telnet

Syntax: show ip telnet

This command shows you the Telnet configuration settings. Command output resembles the following example.

```
Console# show ip telnet
IP Telnet Configuration:

Telnet Status: Enabled
Telnet Service Port: 23
Telnet Max Session: 8
```

Use the **show users** command to display the number of open Telnet sessions at any given time, including information about each session.

Configuration notes

- You can use the **authentication login** command to select a sequence of authentication methods for each type of access to a device (CLI through Telnet, CLI Normal Exel and CLI Privileged Exec levels). Use the **authentication enable** command to specify the sequence of authentication methods to use when changing from Normal Exec command mode to Privileged Exec command mode with the **enable** command.

SNTP

The Simple Network Time Protocol (SNTP) server enables the device to synchronize its clock with an upstream time server. The SNTP server also allows the Brocade device to function as an SNTP server to its downstream clients.

SNTP show commands

show sntp

Syntax: show sntp

This command displays information about the SNTP server.

```
Console# show sntp
Current Time   : Nov 5 18:51:22 2006
Poll Interval  : 16 seconds
Current Mode   : Unicast
SNTP Status    : Enabled
SNTP Server    : 137.92.140.80 0.0.0.0 0.0.0.0
Current Server : 137.92.140.80
```

Chapter

Forwarding Diagnostics 7

This chapter describes diagnostics for forwarding protocols and environments on Brocade BR6910 series switches.

Trunking

Trunk groups are manually-configured aggregate links containing multiple ports. Trunk groups enable load sharing of traffic, and they also provide redundant, alternate paths for traffic if any of the segments fail.

Trunking show commands

Trunk group configuration information can be displayed.

show interfaces status port-channel

Syntax: show interfaces status port-channel *channel-id*

This command displays information about the interface settings and the operation status of a trunk.

```
Console# show interfaces status port-channel 1
Information of Trunk 1
 Basic Information:
  Port Type              : 1000T
  MAC Address            : 70-72-CF-32-DE-09
 Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm        : Enabled
  Broadcast Storm Limit  : 64 Kbits/second
  Flow Control           : Disabled
  VLAN Trunking          : Disabled
  Port Security          : Disabled
  Max MAC Count          : 0
  Port Security Action   : None
 Current Status:
  Created By             : LACP
  Link Status            : Up
  Port Operation Status  : Up
  Operation Speed-duplex : 100full
  Up Time                : 0w 0d 0h 2m 37s (157 seconds)
  Flow Control Type      : None
  Member Ports           : Eth1/11, Eth1/12
```

show lacp counters

Syntax: show lacp *channel-id* counters

This command displays information about the LACP packets sent and received by this trunk.

Command output resembles the following example.

```
Console# show lacp 1 counters
Port Channel : 1
-------------------------------------------------------------------------------
Eth 1/11
-------------------------------------------------------------------------------
  LACPDUs Sent         : 36
  LACPDUs Received     : 30
  Marker Sent          : 0
  Marker Received      : 0
  LACPDUs Unknown Pkts : 0
  LACPDUs Illegal Pkts : 0
  ...
```

show lacp internal

Syntax: show lacp *channel-id* internal

This command displays information about the configuration settings and the operational state for the local side of this trunk.

Command output resembles the following example.

```
Console# show lacp 1 internal
Port Channel : 1
-------------------------------------------------------------------------------
Oper Key  : 3
Admin Key : 0
Eth 1/11
-------------------------------------------------------------------------------
  LACPDUs Internal     : 30 seconds
  LACP System Priority : 32768
  LACP Port Priority   : 32768
  Admin Key            : 3
  Oper Key             : 3
  Admin State          : defaulted, aggregation, long timeout, LACP-activity
  Oper State           : distributing, collecting, synchronization, aggregation,
                         long timeout, LACP-activity
  ...
```

show lacp neighbors

Syntax: show lacp *channel-id* neighbors

This command displays information about the configuration settings and the operational state for the remote side of this trunk.

Command output resembles the following example.

```
Console# show lacp 1 neighbors
Port Channel 1 neighbors
-------------------------------------------------------------------------------
Eth 1/11
-------------------------------------------------------------------------------
  Partner Admin System ID   : 32768, 00-00-00-00-00-00
  Partner Oper System ID    : 32768, 00-E0-0C-00-00-FA
  Partner Admin Port Number : 11
```

```
  Partner Oper Port Number  : 3
  Port Admin Priority       : 32768
  Port Oper Priority        : 32768
  Admin Key                 : 0
  Oper Key                  : 3
  Admin State               : defaulted, distributing, collecting,
                              synchronization, long timeout,
  Oper State                : distributing, collecting, synchronization,
                              aggregation, long timeout, LACP-activity
  ...
```

show lacp sysid

Syntax: show lacp sysid

This command displays a summary of the system priority and MAC address for all channel groups.

Command output resembles the following example.

```
Console# show lacp sysid
Port Channel     System Priority    System MAC Address
--------------------------------------------------------------------------------
           1              32768     70-72-CF-32-DD-FD
           2              32768     70-72-CF-32-DD-FD
           3              32768     70-72-CF-32-DD-FD
           4              32768     70-72-CF-32-DD-FD
           5              32768     70-72-CF-32-DD-FD
           6              32768     70-72-CF-32-DD-FD
           7              32768     70-72-CF-32-DD-FD
           8              32768     70-72-CF-32-DD-FD
           9              32768     70-72-CF-32-DD-FD
          10              32768     70-72-CF-32-DD-FD
          11              32768     70-72-CF-32-DD-FD
          12              32768     70-72-CF-32-DD-FD
```

Configuration notes

There are several trunk group rules. For a full description of these trunking rules, refer to the *Brocade 6910 Ethernet Access Switch Configuration Guide*.

- You can use both static trunk groups and 802.3ad trunking on the same device. However, you can use only one type of trunking for a given port. For example, you can configure port 1/1 as a member of a static trunk group or you can enable 802.3ad link aggregation on the port, but you cannot do both.
- The ports in a trunk group make a single logical link. Therefore, all the ports in a trunk group must be connected to the same device at the other end.
- If you connect physical cables before configuring the trunk groups and then reboot, traffic on the ports can create a spanning tree loop.

Common diagnostic scenarios

Trunk transaction failed; ports overlap with other trunks.

With a static trunk, you must first remove the existing trunk and reconfigure a new one. If you are using dynamic trunk configuration, you would be able to add a port dynamically in the trunk.

Diagnostic Command Index

C

CFM
- maintenance end point, *30*
- maintenance intermediate point, *30*

M

maintenance end point, CFM, *30*
maintenance intermediate point, CFM, *30*

P

ping, *10*
ping6, *10*

S

show access-list, *37*
show access-list tcam-utilization, *5*
show alarm-status, *4*
show dot1x, *41*
show dot1x interface, *42*
show dot1x statistics, *43*
show interfaces brief, *14*
show interfaces counters ethernet, *14*
show interfaces status, *27*
show interfaces status ethernet, *15*
show interfaces status port-channel, *53*
show interfaces switchport ethernet, *16*
show interfaces transceiver, *9*
show ip telnet, *51*
show lacp counters, *54*
show lacp internal, *25*, *54*
show lacp neighbors, *25*, *54*
show lacp sysid, *55*
show log, *1*
show mac-address-table, *20*
show memory, *7*
show port monitor, *45*
show process cpu, *6*
show qos map cos-dscp, *38*
show qos map dscp-mutation, *39*
show qos map phb-queue, *39*
show qos map trust-mode, *38*
show queue mode, *40*
show queue weight, *40*
show radius-server, *46*
show snmp, *47*
show snmp engine-id, *48*
show snmp group, *48*
show snmp user, *49*
show sntp, *52*
show spanning-tree, *21*, *44*
show system, *3*, *7*
show tacacs-server, *49*
show users, *46*, *50*
show version, *4*

T

traceroute, *11*